A secure cryptographic algorithm against side channel attacks

ABSTRACT

Historically, a computing resource is scarce and expensive. In the last few decades, considerable efforts have been made to design efficient codes in terms of the storage space and running time. Due to the progress on computing resources and low cost of memory, an efficient algorithm has ironically become a vulnerable threat to cryptographic operations. An efficient unbalanced code opens another room for side channel attacks on the private key of public key infrastructure (PKI). This paper shall highlight and propose balanced secure algorithms for cryptographic operations to avoid feasible side channel attacks in the immediate future.

Keyword: Side channel attacks; Secure programming